

Data processing device with data processing means utilizing a characteristic value and with means for counteracting analysis methods for the detection of the characteristic value

BACKGROUND OF THE INVENTION

The invention relates to a data processing device which includes a circuit which consists of various circuit sections which can be fed with a supply voltage via a configuration of conductors, and includes data processing means which constitute such a circuit section that can be fed with the supply voltage and are arranged to process data while utilizing a
5 characteristic value, and also includes sequencing means which also constitute such a circuit section that can be fed with the supply voltage and are arranged to execute an algorithm in order to control the data processing means in conformity with this algorithm, which algorithm comprises a given number N of sub-algorithms which contain identical sequences of algorithm steps and can be executed in a given order each time when the algorithm is executed, and
10 wherein, upon processing of data by means of the data processing means under the control of the sequencing means in conformity with the algorithm, the data processing causes a current peak pattern to occur at the area of the configuration of conductors, the pattern configuration of the current peak pattern being dependent on the algorithm steps, on the processed data and on the characteristic value.

The invention also relates to a circuit for a data processing device which consists of various circuit sections which can be fed with a supply voltage via a configuration of conductors and includes data processing means which constitute such a circuit section that can be fed with the supply voltage and are arranged to process data while utilizing a
15 characteristic value, and also includes sequencing means which also constitute such a circuit section that can be fed with the supply voltage and are arranged to execute an algorithm in order to control the data processing means in conformity with this algorithm, which algorithm comprises a given number N of sub-algorithms which contain identical sequences of algorithm steps and can be executed in a given order each time when the algorithm is executed, and
20 wherein, upon processing of data by means of the data processing means under the control of the sequencing means in conformity with the algorithm, the data processing causes a current
25 peak pattern to occur at the area of the configuration of conductors, the pattern configuration

090524 073009
000000 123456

of the current peak pattern being dependent on the algorithm steps, on the processed data and on the characteristic value.

5 A data processing device of the kind set forth in the first paragraph and a circuit of the kind set forth in the second paragraph are known notably from the contact-type chip cards which are used in a variety of versions and include an integrated component developed and marketed by Applicant. In the known data processing device, so in the known contact-type chip card, and in the known circuit, so in the integrated component included in such a known
10 contact-type chip card, the data processing means are formed by encryption means which perform, in conformity with the "Data Encryption Standard" (DES), an encryption operation on data applied thereto while utilizing a characteristic value which is also applied thereto, that is to say a secret key. During such an encryption operation overall $N = 8$ so-called SBOX units are executed, an SBOX result being calculated by means of each SBOX unit. All eight SBOX
15 units are executed within the framework of a program which constitutes an algorithm and each program block of which forms a sub-algorithm and corresponds to an SBOX unit. Each program block, corresponding to an SBOX unit, contains a table which is characteristic of the relevant SBOX unit and contains entries, the entries of all SBOX units being different. The table contained in an SBOX unit, or the entries in this table, is used to determine output data
20 associated with the input data applied to an SBOX unit. Such determination of output data associated with input data, however, is performed while utilizing the same algorithm for the linking of input data and output data in all eight SBOX units; this means that each of the N program blocks, representing a respective SBOX unit and constituting a respective sub-algorithm, contains identical sequences of program instructions as algorithm steps. In the
25 known data processing device, or the known circuit, the N program blocks are invariably executed in the same order each time when the program is executed.

During execution of an encryption operation a current peak pattern occurs at the area of the configuration of conductors, which peak pattern is dependent on the program instructions, on the data processed in the encryption means and on the characteristic value
30 used in the encryption means, so on the secret key for these encryption means. In the known data processing device, or in the known circuit, a problem is encountered in that the respective current peak patterns thus caused also occur in parts of the circuit, or parts of the data processing device, which can be externally interrogated. The occurrence of the respective current peak patterns each time caused in said parts can be used, for example, to supply the

data processing means for the processing of data while utilizing a characteristic value with given known data an arbitrary number of times in succession in order to carry out processing, and to subject the current peak pattern thus produced, always being the same, during the processing of this known data, to observation or detection, so that information concerning the characteristic value, so the secret key, used in the data processing means, so the encryption means, can be extracted from the detected current peak pattern while using rather complex correlation methods or comparison methods which, however, are known and available. Evidently, such cracking of a secret key is undesirable, because the desired secrecy can then no longer be reliably ensured.

SUMMARY OF THE INVENTION

It is an object of the invention to avoid the described problems and to provide, while using simple means and only very little additional work, an improved data processing device, or an improved circuit for a data processing device, which ensures a high degree of reliability in respect of keeping a characteristic value secret.

In order to achieve the described object, a data processing device of the kind set forth in the first paragraph according to the invention is characterized in that the circuit additionally includes order fixation means which co-operate with the sequencing means and whereby, upon each execution of the algorithm, an order can be fixed from a plurality of feasible orders for the execution of the N sub-algorithms.

In order to achieve the described object, furthermore, a circuit of the kind set forth in the second paragraph according to the invention is characterized in that the circuit additionally includes order fixation means which cooperate with the sequencing means and whereby, for each execution of the algorithm, an order can be fixed from a plurality of feasible orders for the execution of the N sub-algorithms.

By taking the steps according to the invention, it is very simply and reliably achieved that even though the succession of all algorithm steps of all successively executed sub-algorithms is always the same for each execution of the algorithm, the order for the execution of the N sub-algorithms of an algorithm is different for each execution of the algorithm, so that the order of the execution of the N sub-algorithms cannot be determined from outside the data processing device or the circuit of the data processing device. Therefore, it is also impossible to compare successively produced current peak patterns, caused by successive activation of the algorithm, in order to use these peak patterns for analysis by means of correlation methods or comparison methods. Undesirable recognition or detection of

a characteristic value used in the data processing means, such as a secret key, thus becomes practically impossible or at least drastically more difficult.

The steps disclosed in the Claims 2 and 3 or 7 and 8 have proven to be very effective for data processing according to the invention, or for a circuit according to the invention, because these embodiments are characterized by a pronounced simplicity and can be readily implemented while using means already present in a data processing device according to the invention or a circuit according to the invention. As regards the order selection means it is to be noted that these order selection means preferably contain only a part of all feasible orders for the execution of the N algorithms, but that it is also simply possible to provide the order selection means with all feasible orders for the execution of N sub-algorithms.

It has been found that the steps according to the invention are particularly advantageously taken in a data processing device in conformity with Claim 4 or a circuit as claimed in Claim 9, because there is a very pronounced need for secrecy as regards the key used notably in the case of means for the encryption and/or decryption of data.

A data processing device according to the invention may be formed, for example by a computer or a personal computer arranged, for example to execute an encryption program. The steps according to the invention have proved to be very attractive notably for a data processing device as disclosed in Claim 7 or in a circuit as disclosed in Claim 14, because the risk of cracking of a characteristic value is particularly high in these cases.

These and other aspects of the invention will become apparent from the embodiment described hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described in detail hereinafter with reference to an embodiment as shown in the drawings, however, without the invention being restricted thereto.

Fig. 1 shows a block diagram of an in this context essential part of a data processing device and a circuit for this data processing device in a first embodiment of the invention.

Fig. 2 shows diagrammatically three executions of one and the same program which consists of a total of N program blocks.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS 21.06.1999

Fig. 1 shows a block diagram of a part of a data processing device which is in this case formed by a data carrier 1 which is constructed for contactless communication with a write/read station which is provided for this purpose but not shown in Fig. 1.

The data carrier 1 includes a circuit 2 which is realized in integrated technology. The circuit 2 consists of a plurality of circuit sections which will be described in detail hereinafter. The circuit sections can be supplied with a supply voltage V via a configuration of conductors 3, said supply voltage being a DC supply voltage. The generating of the supply voltage V will also be described in detail hereinafter.

The data carrier 1 includes transmitter/receiver means 4 which include a transmitter coil 5. The receiver/transmitter means 4 are connected to a first connection 6 and to a second connection 7 of the circuit 2. The transmitter coil 5 can be inductively coupled to a transmitter coil of a write/read station not shown. These two transmitter coils enable a non-modulated carrier signal CS as well as an amplitude modulated carrier signal CSM, being amplitude modulated in conformity with data DA to be transmitted from the write/read station to the data carrier 1, as well as a load modulated carrier signal CSB, which can be generated by means of load modulation means (not shown in Fig. 1) of the data carrier 1, or the circuit 2 of this data carrier 1, and whereby data to be transmitted from the data carrier 1 to a write/read station can be transmitted, to be transmitted between the two communicating partners, so a write/read station and the data carrier 1. The foregoing are facilities which have since long been known.

The supply voltage V can be obtained in the data carrier 1 by means of the non-modulated carrier signal CS transmitted from a write/read station to the data carrier 1 and by means of the amplitude modulated carrier signal CSM transmitted from a write/read station to the data carrier 1. To this end, the non-modulated carrier signal CS received by the receiver/transmitter means 4 and the amplitude modulated carrier signal CSM are applied, via the first connection 6 and an electrically conductive connection 8 connected to the first connection 6, to supply voltage generating means 9. The supply voltage generating means 9 essentially consist of a rectifier stage and a storage capacitor as well as voltage-limiting means which prevent an undesirable overvoltage. The supply voltage generating means 9 are capable of generating the already mentioned supply voltage V which can be output to the configuration of conductors 3 via an output 10 of the supply voltage generating means 9. The generated supply voltage V can be applied to the various circuit sections of the circuit 2 via the configuration of conductors 3. It is to be noted that this configuration of conductors 3 also

includes conductive ground connections which, however, have been omitted in Fig. 1 for the sake of simplicity.

The data carrier 1, or the circuit 2, includes first data processing means 11 which can be supplied with the supply voltage V via a supply input 12. Furthermore, via a connection 13A the first data processing means 11 can also be supplied with the amplitude modulated carrier signal CSM output by the receiver/transmitter means 4. The load modulated carrier signal CSB can be obtained in the receiver/transmitter means 4 by way of the first data processing means 11, via a further connection 13B which is connected to the second connection 7. Furthermore, a first BUS connection 14, connected to sequencing means 15, is connected to the first data processing means 11. The sequencing means 15 are arranged to execute a first algorithm in order to control the first data processing means 11 in conformity with this first algorithm.

The first data processing means 11 include demodulation means (not shown) whereby the applied amplitude modulated carrier signal CSM can be demodulated. After such demodulation of the amplitude modulated carrier signal CSM, if necessary, the demodulated signal can be decoded. If desired, further processing operations may also be performed. After the execution of all processing operations, the first data processing means 11 output data DA via a second BUS connection 16 which is connected to second data processing means 17.

The second data processing means 17 are arranged to process data DA while using a characteristic value CV. In the present case the second data processing means 17 are formed by means for the encryption and/or decryption of data, the secret key required for the encryption and decryption being formed by the previously mentioned characteristic value CV.

The second data processing means 17 include a supply input 18 via which the second data processing means 17 can be supplied with the supply voltage V. Furthermore, a third BUS connection 19 is connected to the second data processing means 17, the other end of said bus connection being connected to the sequencing means 15. The sequencing means 15 are also arranged to execute a second algorithm in order to control the second data processing means 17 in conformity with this second algorithm.

In the present embodiment of the data carrier 1 of Fig. 1 the circuit 2 includes program storage means 20 which co-operate with the sequencing means 15 and in which the second algorithm is stored in the form of a program P. The second algorithm, so the program P, contains a given number N of sub-algorithms which are in this case formed by N program blocks PB1, PB2, PB3 ... PBN. The sub-algorithms, formed by the program blocks PB1 to PBN, contain identical successions of algorithm steps which are formed by program

5

10

25

30

The sequencing means 15 provide control of the second data processing means 17 during the execution of such encryption operations, that is to say essentially in such a manner that the sequencing means 15 successively read the program instructions CO1, CO2 etc., via the fourth BUS connection 21, from the program P stored in the program storage means 20, after which a processing step, corresponding to the respective read program instruction, is executed in the second data processing means 17. During such processing of data DA by means of the second data processing means 17, under the control of the sequencing means 15 in conformity with the program P stored in the program storage means 20, a current peak pattern occurs at the area of the configuration of conductors 3 due to the data processing. The pattern configuration of the current peak pattern is then dependent on the program instructions CO1, CO2 ... COR, on the processed data DA, and on the characteristic value CV.

The data carrier 1, or the circuit 2, is preferably constructed in such a manner that the circuit 2 includes additional order fixation means 29 which co-operate with the sequencing means 15 and whereby, upon each execution of the algorithm formed by the program stored in the program storage means 20, an order can be fixed from a plurality of feasible orders for the execution of the N sub-algorithms; so the N program blocks PB1, PB2 ... PBN.

In the present embodiment the order fixation means 29 include a random number generator 30. The random number generator 30 includes a supply input 31 via which the supply voltage V can be applied to the random number generator 30. The random number generator 30 is connected to the sequencing means 15, via a sixth BUS connection 32. Each random number Z generated by the random number generator 30 can thus be applied to the sequencing means 15 via the sixth BUS connection 32. The order fixation means 29, including the random number generator 30, are capable of fixing, upon each execution of the program P stored in the program storage means 20, an order which is determined by the random number Z generated by the random number generator 30 and is used for the execution of the N program blocks PB1 to PBN of the program P.

To this end, the order fixation means 29 additionally include order selection means 33 which are included in the sequencing means 15. The order selection means 33 contain feasible orders for the execution of the N program blocks PB1 to PBN of the program P. Preferably, the order selection means 33 contain only a part of all feasible orders. The order selection means 33 co-operate with the random number generator 30, that is to say in such a manner that the order selection means 33 can select an order from the feasible orders,

contained in the order selection means 33, in conformity with the random number Z which is received from the random number generator 30 via the sixth BUS connection 32.

The first data processing means 11, the sequencing means 15, the second data processing means 17, the program storage means 20, the storage means 23 and the random number generator 30 constitute a respective circuit section of the circuit 2, which circuit sections can be supplied with the supply voltage V via the configuration of conductors 3.

The operation of the data carrier 1 and the circuit 2, respectively, in respect of the processing of data DA by means of the second data processing means 17 and under the control of the sequencing means 15 in conformity with the program P will be described in detail hereinafter with reference to the program blocks PB1 to PBN in Fig. 2.

It is assumed that in the course of a data processing operation in the data carrier 1, or by means of the circuit 2 of the data carrier 1, the second data processing means 17, being arranged to process data DA while using the characteristic value CV, are successively activated for three data processing cycles which are denoted by the references RUN1, RUN2 and RUN3 in Fig. 2. Before the first data processing cycle RUN1 of the second data processing means 17 is reached in the course of such a data processing operation, the random number generator 30 is activated in a manner not described, after which the random number generator 30 generates a random number Z1 which is applied to the order selection means 33 via the sixth BUS connection 32. The order selection means 33 then select, in conformity with the random number Z1 received from the random number generator 30, an order for the execution of the N program blocks PB1 to PBN of the program P, for example the order PB1, PB2, PB4, PB6, PB3, ... PB5 and PBN shown in the left-hand column in Fig. 2. Subsequently, the program blocks PB1 to PBN are executed in the described order. All program instructions CO1, CO2, ... COR, CO1, CO2, ... COR etc. until CO1, CO2 ... COR contained in said program blocks are executed; this means that the successive program instructions CO1, CO2 to COR overall are executed N times in succession as indicated in the right-hand column of Fig. 2.

When the second data processing cycle RUN2 is to be executed during the data processing operation, first the random number generator 30 is activated again, with the result that the random number generator 30 outputs a second random number Z2. The second random number Z2 is applied, via the sixth BUS connection 32, to the order selection means 33 so that the order selection means select a further order, for example the order PB6, PB3, PB7, PBN, PB1, ... PB4 and PB2 shown in the second column of Fig. 2. Thus, the second data processing cycle RUN2 involves a completely different order for the execution of the N

program blocks. The order of the program instructions CO1, CO2 to COR etc., however, remains the same.

When the third data processing cycle RUN3 is to be executed in the course of the assumed data processing operation, the random number generator 30 is activated again in the same way as described above, so that the generator generates the random number Z3 and applies it, via the sixth BUS connection 32, to the sequencing means 15 or the order selection means 33 included therein. Consequently, the order selection means 33 select a further order for the execution of the N program blocks PB1 to PBN, for example the order PBN, PB1, PB4, PB6, PB3, ... PB7 and PB2 shown in the third column of Fig. 2. The third data processing cycle RUN3 thus involves a new order again for the execution of the N program blocks PB1 to PBN of the program P, the order of the program instructions CO1, CO2 to COR etc., however, again being the same.

As will be evident from the foregoing description, for the data carrier 1 shown in Fig. 1, or for the circuit 2 of the data carrier 1, it is achieved that, even though the order of all program instructions COX of all successively executed program blocks PBX is always the same upon each execution of the program P, the order for the execution of the N program blocks PBX of the program P is different during each execution of this program. It is thus achieved that the order of the execution of the N program blocks PBX cannot be detected from outside the data carrier 1 or the circuit 2 of the data carrier 1. Consequently, it is also impossible to compare successive orders of current peak patterns, caused by successive activation of the program P, in order to use such orders for analysis utilizing correlation methods, or to use the order of occurrence of the N current peak patterns, one of which occurs upon each execution of a program block PBX, for comparison methods. It is thus achieved that undesirable detection or recognition of the characteristic value CV used in the second data processing means 17 is practically impossible.

A further embodiment of data carrier (not shown) is provided with a wired logic circuit instead of the program storage means 20; this wired logic circuit co-operates with the sequencing means 15 and contains a wired algorithm, i.e. a hardware algorithm. This algorithm, stored hardware-wise in the wired logic circuit, enables analogous control of the second data processing means 17 by means of the sequencing means 15.

The invention is not restricted to the data processing device, so the data carrier 1, in the embodiment shown in and described with reference to Fig. 1. In the data carrier 1 shown in Fig. 1 the order selection means 33 are constructed so as to form part of the sequencing means 15, the order selection means 33 being realized in hardware. In a further

5
10

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1